IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ROSALINDA.1031@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 3:24-sw- 38

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Daniel E. Leary, a Special Agent with Homeland Security Investigations, Department of Homeland Security, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the above-listed Apple ID stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Your affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I am a Special Agent with the Richmond, Virginia, office of the Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and have been employed as a Special Agent since July 2003. I am currently a member of the Richmond Division Child Exploitation Task Force and have been since March 2018. I have participated in investigations involving sexual assaults, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18 of the United States Code, involving child exploitation offense.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including child exploitation offenses.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2423(a) (transportation of a minor with intent to engage in criminal sexual activity), 18 U.S.C. §1591 (sex trafficking of a minor); and 18 U.S.C. § 2251(a) (production of child pornography) have been committed by Daniel Kidd and Rosalinda Rosas. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court "a district court of the United States . . . that has jurisdiction over the offense being investigated."

FACTUAL BACKGROUND

7. In April 2022, a joint investigation initiated by the Powhatan County Sheriff's Office and HSI revealed that ROSALINDA DELGADO ROSAS ("ROSAS") and DANIEL WAYNE KIDD ("KIDD") were involved in the transportation of a 15-year-old child ("Minor Victim 1" or "MV1") from Michigan to Virginia and the subsequent repeated sexual abuse of MV1.

8. Specifically, on April 8, 2022, Powhatan County Sheriff's Office received a call from Laura Piechoksi, a nurse employed at Helen DeVos Children's Hospital in Grand Rapids

Michigan. Nurse Piechoski reported the rape of a 15-year-old child that occurred in Powhatan County, Virgina on or about April 1, 2022, through on or about April 7, 2022.

9. Investigation verified that on April 1, 2022, ROSAS flew from Richmond, Virginia to Michigan to transport MV1 to Virginia for the week of April 1 through April 7. On April 8, 2022, ROSAS flew from Richmond, Virginia to Michigan to return MV1 to Michigan (MV1's home state). On April 8, MV1 was picked up from the airport by her stepfather. ROSAS did not remain in Michigan and returned immediately to Virginia.

10. Upon entering her stepfather's car outside of the airport, MV1 began to cry, hugged her stepfather, and disclosed that KIDD had sexually abused her each night of her stay in Virginia. MV1 made disclosures to family and to law enforcement. MV1 disclosed that KIDD both vaginally and orally raped her. She also disclosed that ROSAS was present for the rapes and watched them. MV1 disclosed that the rapes occurred in the home of KIDD and ROSAS in Powhatan County, Virginia—specifically the bedroom of ROSAS and KIDD and occasionally beginning in the living room. MV1 also disclosed during her sexual assault examination that one evening in the middle of the night KIDD woke MV1 in the room she was sleeping in and began to molest her. MV1 stated that she observed cameras in the living room as well as other parts of the home, and was aware there was a camera in the room she was sleeping in. MV1 stated that the cameras in the house were connected to ROSAS' and KIDD's phones. MV1 explained that at times while KIDD was sexually abusing MV1, MV1 observed ROSAS checking her phone. ROSAS previously informed MV1 that she would watch the security cameras to ensure that the ROSAS's son remained in his room and did not discover or observe the sexual abuse. MV1 stated that ROSAS and KIDD bought her several expensive gifts including, Apple AirPods, an Apple Watch, and nice clothes to keep quiet.

11. On April 8, 2022, a sexual assault kit was conducted on MV1 at YWCA West Central in Grand Rapids, Michigan. Stephanie Solis, the Nurse Examiner Program Manager, reported that bruising was observed on MV1 on her groin area, right outer thigh, above her left knee, left thigh, and inner calf. She also reported that MV1 suffered trauma to three areas on the right side of the vagina where circular red abrasions were observed. Solis identified abrasions on the inner wall of the vagina that were observed through the use of dye on MV1.

12. A child forensic interview was conducted on MV1. In the interview MV1 explained that while in transit to Virginia, but prior to arriving at ROSAS' and KIDD's residence (the "Residence"), ROSAS began telling MV1 that KIDD was sexually interested in MV1 and that ROSAS wanted MV1 to tease KIDD to see how long it would take him to do something sexual to MV1. ROSAS also told MV1 that KIDD was going "spoil her."[1] The evening MV1 arrived at KIDD's Residence, MV1 showered and entered the living room where she laid on the couch and KIDD began to touch her under her clothes including her vaginal area. ROSAS was present and watched. MV1 was then taken into ROSAS and KIDD's bedroom where she undressed and KIDD and MV1 engaged in oral sex while ROSAS watched. Throughout the week KIDD engaged in oral and vaginal sex with MV1. ROSAS was often present and watched. She also instructed MV1 on how to perform oral sex on KIDD. At some point in the week, KIDD also choked and slapped MV1 while having sex with her.

---

[1] Your Affiant understands this to mean that KIDD was going to purchase many things and experiences for MV1.

13. ROSAS' minor son was also present in the Residence for the week of April 1 through April 8. At some point during the week, while at an amusement park MV1 disclosed to ROSAS' son that KIDD had been having sex with MV1 and ROSAS was aware of it.

14. On April 12, 2022, Powhatan County Sheriff's Office obtained a warrant to search ROSAS' and KIDD's Residence. The search warrant authorized the seizure of electronic devices. Numerous items were seized, including an iPhone 13 determined to belong to ROSAS ("ROSAS' iPhone").

15. On April 13, 2022, law enforcement conducted a non-custodial interview of ROSAS' minor son. ROSAS' son confirmed that MV1 had visited and stayed in the Residence from April 1 through April 8. He also stated that during her visit, MV 1 disclosed to him, while at an amusement park, that KIDD was having sex with MV1. ROSAS' son also stated that soon after MV1 left Virgina he disclosed to his mom, ROSAS, that MV1 had told him that KIDD had sex with MV1 and ROSAS was aware of it.

16. On April 13, 2022, law enforcement conducted non-custodial interviews of KIDD and ROSAS. Both ROSAS and KIDD confirmed, in their respective interviews, that MV1 was present in the Residence from April 1 through April 8. They also confirmed that several gifts were given to MV1 including an Apple Watch, Apple AirPods, clothing from Target, trips to Kings Dominion, and several meals out. They also confirmed that MV1 stayed in the room on the first floor that KIDD's daughter uses when she stays at the Residence. Both confirmed cameras are in the room MV1 stayed in as well as the living room. KIDD confirmed that the camera system in the house including the cameras in the living room and the room MV1 stayed in are Google Nest. He also confirmed that the cameras sync to his phone and videos are retained for 60 days. From my review of publicly available information provided by Nest about

its services, including Nest's "Privacy Policy" and "Terms of Service," I am aware of the following about Nest. Nest cameras are used to capture still images and video footage for a variety of purposes including home monitoring. Nest cameras connect to the internet and provide users the ability to monitor the camera in real time, as well as to save and store video recording if certain features and subscription services are enabled. Users can access this video feed through Google's mobile application or other third-party applications.

17. ROSAS iPhone is currently in the lawful possession of the United States. Pursuant to the state search warrants, ROSAS' iPhone was forensically imaged by and reviewed by law enforcement.

18. Review of the forensic images revealed short video snippets captured by the Google Nest camera in the room in which MV1 stayed when she was in the residence with KIDD and ROSAS. These video snippets were found on ROSAS' iPhone from the week of April 1 to 8 when MV1 stayed in the residence with KIDD and ROSAS. On several of these videos, KIDD can be seen in the room with MV1. According to exif data, these videos were captured at late hours of the night and or early hours of the morning. In certain of the videos both KIDD and or MV1 are in various states of undress on or around the bed. Several of the videos feature KIDD in positions indicative of him engaging in sexual acts with MV1. These video snippets were found on ROSAS' iPhone in a folder associated with the Google Nest application. Forensic review further showed that the user of ROSAS' iPhone accessed the Nest application frequently during the nights that MV1 was sexually abused during the approximate time periods that MV1 was sexually abused.

19. Images found elsewhere on ROSAS' iPhone also appear to be associated with the Google Nest camera. Specifically, images in the residence were found that bear the logo "Nest,"

appear to show the Nest application, and at least one is identifiable as the same general camera angle as shown in the video snippets described above. Based on my review of these images, it appears as though they are user-generated screenshots of the Nest application. These can occur when a user is either watching the live feed of a Nest camera or reviewing stored footage and then takes a screenshot of what they are viewing. One of these images appears to show KIDD and ROSAS engaging in sexual activity in the same room that video snippets of MV1's sexual abuse were captured. These screenshots were located in a folder on ROSAS' iPhone titled "CPLAssets." I know based on speaking to a forensic examiner that the existence of the folder CPLAssets on the device means that Apple iCloud was used to store or view the images contained in the folder.

20. Also located on ROSAS' iPhone are thumbnail versions of the Nest screenshots described above. After speaking with a forensic examiner, I was informed that because there are thumbnail versions of the original files and the original files themselves located on the device, that means the original versions of the files were stored in the iCloud and viewed on the device.

21. The CPLAssets folder on ROSAS' iPhone also contained images of MV1 that are unrelated to the Nest camera. For example, there are images that appear to be screenshots of a social media account belonging to MV1, images of MV1 from around the first time she met KIDD, and images of MV1 from when she was younger.

22. Other images related to MV1's trip to Virginia for the week of April 1 through April 8 were also identified on ROSAS' iPhone. These images include pictures of MV1 in Virgina and in transit from Michigan to Virginia.

23. Internet history and search history relevant to the investigation were also identified on ROSAS' iPhone. These included, but were not limited to, searching for items

purchased for MV 1 and stores that MV1 was taken to purchase items for MV1 close in time to when MV1 was taken to those stores. For example, the user searched for "chesterfield mall victoria's secret" close in time to when MV1 was taken to those stores and items were purchased for her, including lingerie. I know based on speaking to a forensic examiner, that other internet activity coincides with the approximate time of night MV1 was sexually abused by KIDD and MV1 reported that ROSAS was periodically on her phone. This includes a search for "lorazapam and not being erect". The forensic examination of ROSAS' iPhone also found numerous relevant messages. For example, iMessage communications between KIDD and ROSAS were identified wherein they discuss MV1 after they have been informed of her outcry by the other minor in the home were also identified on ROSAS' iPhone. iMessage communications between ROSAS and MV1's parents related to MV1's trip to Virginia were also identified on ROSAS' iPhone.

24. Law enforcement was provided images of electronic communications between ROSAS and MV1 on the social media application "Instagram". These communications include the planning of MV1's trip to Virginia and ROSAS' describing ways that KIDD and ROSAS were going to "spoil" MV1. These images were identified and captured by MV1's mother after MV1 disclosed the sexual abuse. These images reflect conversations between ROSAS and MV1 on Instagram dating back to January 29, 2022.

25. The forensic review of ROSAS' iPhone identified that the Apple ID registered on the device was ROSALINDA.1031@GMAIL.COM ("SUBJECT ACCOUNT"). ROSAS' stated in her noncustodial interview, that she had recently upgraded her phone to an iPhone 13. The forensic review of ROSAS' iPhone identified an email from Apple to ROSALINDA.1031@GMAIL.COM dated March 29, 2022, which notified the user of

SUBJECT ACCOUNT that the SUBJECT ACCOUNT Apple user ID had been used to sign into an iPhone 13.

26. I know based on speaking to a forensic examiner that the person using the Apple ID of SUBJECT ACCOUNT downloaded the Instagram app onto ROSAS' iPhone on approximately March 29, 2022.

27. I know based on speaking to a forensic examiner that the person using the Apple ID of SUBJECT ACCOUNT downloaded the Nest app onto ROSAS' iPhone that same day. I know based on speaking to a forensic examiner that ROSAS' iPhone was backed up to iCloud including as recently as April 12, 2022, the day before the phone was seized.

BACKGROUND CONCERNING APPLE[2]

28. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

29. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

---

[2] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their

location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

30. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

31. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

32. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

33. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

34. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

35. This is an investigation into the transportation of a minor with the intent to engage in criminal sexual activity as well as the sex trafficking of a minor and production of child pornography. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

36. The evidence described above in paragraphs 14-26 indicates that the user of ROSAS' iPhone backed up the phone to the iCloud and the contents of the phone contain relevant evidence to this investigation and that additional evidence may have been backed up and saved to the iCloud. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

37. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and

because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

38. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

39. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of instrumentalities of the crimes under investigation.

40. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

41. Based on the foregoing, I request that the Court issue the proposed search warrant.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Daniel E. Leary
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on February 27, 2024.

/s/

Honorable Summer L. Speight
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with ROSALINDA.1031@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI") **from January 1, 2022 to April 12, 2022;**

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments **from January 1, 2022 to April 12, 2022;**

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message **from January 1, 2022 to April 12, 2022;**

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks **from January 1, 2022 to April 12, 2022;**

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades **from January 1, 2022 to April 12, 2022**;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps **from January 1, 2022 to April 12, 2022**;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2423(a) (transportation of a minor with intent to engage in criminal sexual activity), 18 U.S.C. §1591 (sex trafficking of a minor); and 18 U.S.C. § 2251(a) (production of child pornography) those violations involving KIDD and ROSAS from January 1, 2022 to April 12, 2022 including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence of sexual exploitation of MV1;

b. Evidence of the production of child pornography;

c. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

d. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

e. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

f. The identity of the person(s) who communicated with the user ID about matters relating to MV1 including records that help reveal their whereabouts.